

Remarks:

This amendment and these remarks are responsive to the non-final Office action dated October 6, 2005, and are being submitted under 37 C.F.R. § 1.111. Claims 1-30 are pending in the application. In the Office action, the Examiner rejected claim 12 under 35 U.S.C. § 112, second paragraph, as being indefinite, and rejected claims 1-30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,373,551 to Manico et al. ("Manico") in view of "Applied Cryptography," pages 31-41, by Bruce Schneier ("Schneier"). Applicants traverse the rejections, contending that each of rejected claims 1-30 is not indefinite, anticipated, or obvious.

Nevertheless, to expedite the issuance of a patent, and to more particularly point out and distinctly claim aspects of the invention that applicants would like to patent now, applicants have amended claim 12. However, applicants reserve the right to prosecute this claim in its original form at a later time. Furthermore, applicants have presented remarks showing that claims 1-30 are neither taught nor suggested by the cited references. Accordingly, applicants respectfully request reconsideration of the rejected claims, and prompt issuance of a Notice of Allowability covering all of the pending claims.

I. Claims Rejections – 35 U.S.C. § 112

The Examiner rejected claim 12 under 35 U.S.C. § 112, second paragraph, as being indefinite. In particular, the Examiner cited the phrase "at least substantially" as being indefinite. Applicants traverse the rejection, contending that one of ordinary skill in the art would understand the meaning of this phrase in the present context. However, in the interest of expediting prosecution, applicants have amended claim

Page 7 - AMENDMENT
Serial No. 10/086,771
HP Docket No. 10015964-1
KH Docket No. HPCB 334

12 to delete this phrase. Accordingly, applicants believe the Examiner's rejection under 35 U.S.C. § 112 has been addressed fully and should be removed.

II. Claims Rejections – 35 U.S.C. § 103

The Examiner rejected each of the pending claims as being obvious over Manico in view of Schneier. Applicants traverse the rejections, contending that the cited references, either alone or in combination, do not teach or suggest every element of any of the rejected claims. The bases for this contention are set forth below for each of independent claims 1, 13, 18, and 27, and their dependent claims.

A. Claims 1-12

Claim 1 is directed to a method of encrypting an image:

1. (Original) A method of encrypting an image produced from physical information, comprising:
 - digitizing spatially-distributed physical information to create a digital image of the information;
 - digitizing a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key;
 - reading the digital tag to identify the public key; and
 - encrypting the digital image with the identified public key.

Claim 1 is patentable over Manico and Schneier because, for example, these references do not teach or suggest (1) "encrypting the digital image with the identified public key," or (2) "digitizing a physical tag" to create a digital tag "readable to identify a public key."

Manico relates to a system for communicating digital images generated from photographic film. The system involves photographic film (and/or a cassette) having a unique identification code. For example, Figure 2 (reproduced below) of Manico illustrates a film cartridge 70 with respective human and machine-readable ID codes

90, 100. An identification tab is included with the photographic film. For example, Figure 3 of Manico illustrates a mailing envelope 110 with a tear-off tab 120. The tab is imprinted with a unique URL address 130 and a password or "security code" 140. The URL address links the tab to the film ID code. In use, a user takes pictures with the photographic film and then sends the film to a film developer in the mailing envelope, while retaining the tear-off tab. The URL address and security code on the tab then allow the user to access and receive, over a computer network, digital photographs produced from the developed film.

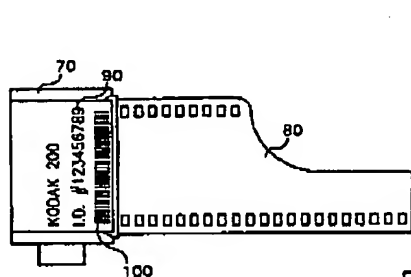


FIG. 2

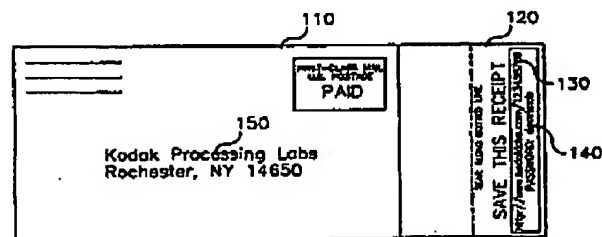


FIG. 3

In the Office action, the Examiner asserted that Manico discloses a method of encrypting an image. Applicants strongly disagree with this assertion. Manico discloses access to digital images over a computer network, with the access being restricted by a password (a security code). However, this restricted access is not disclosed to involve any encryption of the digital images themselves. In other words, providing the security code makes the digital images available to the user, instead of allowing the images to be decoded from an encrypted form.

The Examiner also suggested that the "security code" of Manico identifies a public key. Applicants strongly disagree with this assertion. The security code of Manico does not identify a public key for at least two reasons. First, a public key generally is not kept secret and is available to others (see application, e.g., page 1,

Page 9 - AMENDMENT
Serial No. 10/086,771
HP Docket No. 10015964-1
KH Docket No. HPCB 334

lines 27-30), so that encryption of data with the public key generally is not restricted. In contrast, the security code of Manico is a private access code that is not available to others. Otherwise, the security code of Manico would not provide any security. Second, a public key is a member of an asymmetric pair of keys, such that encryption with the public key allows decoding with the private key, and vice versa. The security code of Manico is not disclosed to identify a public (or private) member of such an asymmetric pair.

In the Office action, the Examiner combined Manico with Schneier and asserted that Schneier "teaches a method of encrypting a digital image using a public key." Applicants disagree. Schneier involves encryption of "messages" and "documents." However, Schneier does not disclose creating digital images produced by "digitizing spatially-distributed physical information," as recited by claim 1. Schneier also does not teach or suggest digitizing a physical tag to create a digital tag, as recited by claim 1.

In summary, neither Manico nor Schneier teaches or suggests every element of claim 1. Claim 1 thus should be allowed. Claims 2-12, which depend from claim 1, also should be allowed for at least the same reasons as claim 1.

B. Claims 13-17

Claim 13 is directed to a method of sending an encrypted image:

13. (Original) A method of sending an encrypted image of a document, comprising:

disposing a physical tag on a document, the physical tag having a code that carries a public key;

digitizing the document to create a digital image that includes a digital representation of the code;

reading the digital representation of the code to obtain the public key;

encrypting the digital image with the obtained public key; and

Page 10 - AMENDMENT
Serial No. 10/086,771
HP Docket No. 10015964-1
KH Docket No. HPCB 334

sending the encrypted image to a recipient that holds a private key, the private key forming a key pair with the public key.

Claim 13 is patentable over Manico and Schneier because neither of these references teaches or suggests every element of claim 13. For example, based on the reasoning presented above in relation to claim 1, these references do not teach or suggest (1) "reading the digital representation of the code to obtain the public key," or (2) "encrypting the digital image with the obtained public key." Claim 13 thus should be allowed. Claims 14-17, which depend from claim 13, also should be allowed for at least the same reasons as claim 13.

C. Claims 18-26

Claim 18 is directed to a device for encrypting an image:

18. (Original) A device for encrypting an image produced from spatially-distributed physical information, the device comprising:

at least one digitizing mechanism adapted to digitize spatially-distributed physical information to create a digital image, and to digitize a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key; and

a processor operatively connected to the digitizing mechanism and adapted to receive the digital image and digital tag from the at least one digitizing mechanism, to read the digital tag to identify the public key, and to encrypt the image with the identified public key.

Claim 18 is patentable over Manico and Schneier because neither of these references teaches or suggests every element of claim 18. For example, based on the reasoning presented above in relation to claim 1, these references do not teach or suggest a processor adapted (1) "to read the digital tag to identify the public key," or (2) "to encrypt the image with the identified public key." Claim 18 thus should be

allowed. Claims 19-26, which depend from claim 18, also should be allowed for at least the same reasons as claim 18.

D. Claims 27-30

Claim 27 is directed to a program storage device:

27. (Original) A program storage device readable by a processor, tangibly embodying a program of instructions executable by the processor to perform method steps for encrypting an image produced from physical information, comprising:

digitizing spatially-distributed physical information to create a digital image of the information;

digitizing a physical tag associated with the physical information to create a digital tag, the digital tag being readable to identify a public key;

reading the digital tag to identify the public key; and

encrypting the digital image with the identified public key.

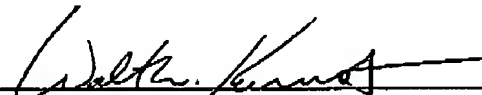
Claim 27 is patentable over Manico and Schneier because neither of these references teaches or suggests every element of claim 27. For example, based on the reasoning presented above in relation to claim 1, these references do not teach or suggest (1) "encrypting the digital image with the identified public key," or (2) "digitizing a physical tag" to create a digital tag "readable to identify a public key." Claim 27 thus should be allowed. Claims 28-30, which depend from claim 27, also should be allowed for at least the same reasons as claim 27.

III. Conclusion

Applicants believe that this application is now in condition for allowance, in view of the above amendments and remarks. Accordingly, applicants respectfully request that the Examiner issue a Notice of Allowability covering the pending claims. If the Examiner has any questions, or if a telephone interview would in any way advance prosecution of the application, please contact the undersigned attorney of record.

Respectfully submitted,

KOLISCH HARTWELL, P.C.



Walter W. Kamstein
Registration No. 35,565
520 S.W. Yamhill Street, Suite 200
Portland, Oregon 97204
Telephone: (503) 224-6655
Facsimile: (503) 295-6679
Attorney for Applicants

CERTIFICATE OF FACSIMILE TRANSMISSION

I hereby certify that this correspondence is being facsimile transmitted to Examiner T. Teslovich, Group Art Unit 2137, Assistant Commissioner for Patents, at facsimile number (571) 273-8300 on November 1, 2005.



Christie A. Doolittle

Page 13 - AMENDMENT
Serial No. 10/086,771
HP Docket No. 10015964-1
KH Docket No. HPCB 334